A CONDITIONAL CONSTRUCTION OF RESTRICTED ISOMETRIES

AFONSO S. BANDEIRA, DUSTIN G. MIXON, AND JOEL MOREIRA

Abstract. We study the restricted isometry property of a matrix that is built from the discrete Fourier transform matrix by collecting rows indexed by quadratic residues. We find an $\epsilon > 0$ such that, conditioned on a folklore conjecture in number theory, this matrix satisfies the restricted isometry property with sparsity parameter $K = \Omega(M^{1/2+\epsilon})$, where M is the number of rows.

1. Introduction

Let $K \leq M \leq N$ be positive integers and let $0 \leq \delta < 1$. An $M \times N$ matrix Φ is said to satisfy the (K, δ)-*restricted isometry property (RIP)* if

$$(1 - \delta)\|x\|^2 \leq \|\Phi x\|^2 \leq (1 + \delta)\|x\|^2$$

whenever $x \in \mathbb{R}^N$ has at most K nonzero entries (i.e., x is a K-sparse vector); here, $\|\cdot\|$ denotes the ℓ_2 norm. RIP matrices are important in signal processing, making it possible to measure and recover a sparse signal using significantly fewer measurements than the dimension of the signal [7]. Random matrices have been shown to satisfy the RIP with high probability for several distributions [5, 9, 11, 12, 13]. However, matrices constructed randomly have a nonzero (albeit small) probability of failing to be RIP, and checking whether a given matrix satisfies this property is an NP-hard problem [2]. This has raised the interest in constructing explicit RIP matrices [14].

While random constructions provide sparsity levels K as high as $O_\delta(M/\operatorname{polylog} N)$, which is essentially optimal [5], most deterministic constructions only achieve $K = O(\sqrt{M})$. The only construction so far to break this square-root bottleneck is due to Bourgain, Dilworth, Ford, Konyagin and Kutzarova [6]; they construct a matrix satisfying RIP with $K = \Omega(M^{1/2+\epsilon})$ for some $\epsilon > 0$. Their analysis has since been optimized to show that ϵ can be taken to be 4.4466×10^{-24} [10]. Some effort has also been made in derandomizing the construction of RIP matrices [3], i.e., finding random constructions of RIP matrices using as few random bits as possible.

The *Paley matrix* is a deterministic matrix constructed using the quadratic residues modulo a prime p; we postpone the precise definition to the next section. In [4], it was conjectured that the Paley matrix satisfies the (K, δ)-RIP for some $K = \Omega_\delta(p/\operatorname{polylog} p)$. In this note, we leverage a folklore conjecture in number theory, Conjecture 2.2 below, which attempts to quantify the pseudorandomness of the Legendre symbol (and hence of the Paley matrix) to prove that the Paley matrix is (K, δ)-RIP with $K = \Omega(M^{1/2+\epsilon})$ for some $\epsilon > 0$. This provides another deterministic construction which breaks the square-root bottleneck, although conditionally on a conjecture.

Key words and phrases. Paley graph, restricted isometry property, Legendre symbol.

ASB was supported by AFOSR Grant No. FA9550-12-1-0317. DGM was supported by NSF Grant No. DMS-1321779. The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

2. The Paley matrix

Throughout this paper we let $p \equiv 1 \bmod 4$ be a prime, let $\mathbb{F}_p$ denote the field with p elements and let $\chi : \mathbb{F}_p \to \{-1, 0, 1\}$ denote the Legendre symbol, defined by

$$\chi(x) = \begin{cases} 1 & \text{if } x = y^2 \text{ for some } y \in \mathbb{F}_p \setminus \{0\} \\ 0 & \text{if } x = 0 \\ -1 & \text{otherwise.} \end{cases}$$

The *Paley graph* is the graph with vertex set $\mathbb{F}_p$ and with an edge between two vertices x and y if and only if $\chi(x - y) = 1$. We now define the *Paley matrix*, denoted by Φ. We use the notation $e(a) := e^{2\pi i a/p}$.

First let $Q = \{x \in \mathbb{F}_p : \chi(x) \geq 0\}$ be the set of squares in $\mathbb{F}_p$, and take $M = |Q| = (p+1)/2$. Construct the $M \times p$ matrix H with entries $H[i, j] = e(-i^2 j)$. In other words, H contains the rows of the discrete Fourier transform matrix indexed by Q. Next let $\tilde{\Phi}$ be the $M \times p$ matrix obtained from H by normalizing its entries so that the entries in the first row of $\tilde{\Phi}$ have absolute value $\sqrt{1/p}$ and the other entries of $\tilde{\Phi}$ have absolute value $\sqrt{2/p}$. Finally, let the Paley matrix Φ be the $M \times 2M$ matrix obtained from the concatenation of $\tilde{\Phi}$ with the first column of the $M \times M$ identity matrix. For instance, the Paley matrix for $p = 5$ is

$$\Phi = \begin{bmatrix} \sqrt{\frac{1}{5}} & \sqrt{\frac{1}{5}} & \sqrt{\frac{1}{5}} & \sqrt{\frac{1}{5}} & \sqrt{\frac{1}{5}} & 1 \\ \sqrt{\frac{2}{5}} & \sqrt{\frac{2}{5}} e^{-2\pi i/5} & \sqrt{\frac{2}{5}} e^{-2\pi i 2/5} & \sqrt{\frac{2}{5}} e^{-2\pi i 3/5} & \sqrt{\frac{2}{5}} e^{-2\pi i 4/5} & 0 \\ \sqrt{\frac{2}{5}} & \sqrt{\frac{2}{5}} e^{-2\pi i 4/5} & \sqrt{\frac{2}{5}} e^{-2\pi i 3/5} & \sqrt{\frac{2}{5}} e^{-2\pi i 2/5} & \sqrt{\frac{2}{5}} e^{-2\pi i/5} & 0 \end{bmatrix}.$$

Interestingly, there exists a 3×3 unitary matrix U such that $U\Phi$ is real, and the lines spanned by the column vectors of $U\Phi$ intersect the real unit sphere at the vertices of an icosahedron; in this way, the Paley matrix generalizes the icosahedron.

One well known construction of a random matrix satisfying the RIP (with high probability) is gotten by extracting a random subset of the rows of the discrete Fourier transform matrix [13]. Thus the claim that Φ satisfies the RIP can be viewed as asserting that the set Q behaves randomly in this sense. This is reasonable, as the Legendre symbol is known to behave pseudorandomly. For instance, in [3], this pseudorandomness was used to produce RIP matrices with entries being consecutive values of χ, using fewer random bits than the usual random constructions.

While currently available results concerning the random-like behavior of χ seem to be insufficient to obtain a deterministic RIP matrix, we will make use of a well known number theoretic conjecture to this end. The following definition will be convenient:

Definition 2.1. *For each of the following, we implicitly take $p \equiv 1 \bmod 4$ to be prime:*

(a) *Let* PaleyDiscrepancy$[\alpha, \beta]$ *denote the statement that for every sufficiently large p,*

$$\left| \sum_{a,b \in S} \chi(a - b) \right| < |S|^{2-\beta} \qquad \forall S \subseteq \mathbb{F}_p \text{ such that } |S| > p^\alpha. \tag{1}$$

(b) *Let* PaleyRIP$[\gamma, \eta]$ *denote the statement that for every sufficiently large p, the $(p+1)/2 \times (p+1)$ Paley matrix satisfies the (p^γ, p^η)-restricted isometry property.*

(c) *Let* PaleyClique$[\tau]$ *denote the statement that for every sufficiently large p, the largest clique in the Paley graph of p vertices has $\leq p^\tau$ vertices.*

The following (folklore) conjecture appeared as Conjecture 2.2 in [8], where a proof for $\alpha > 1/2$ is given; it has also been used in [15] to produce a pseudorandom number generator.

Conjecture 2.2. *For each $\alpha > 0$, there exists $\beta = \beta(\alpha) > 0$ such that* PaleyDiscrepancy$[\alpha, \beta]$.

This particular formulation states that for any subcollection of vertices S in the Paley graph with $|S| > p^\alpha$, the number $e(S)$ of induced edges satisfies

$$\left| e(S) - \frac{1}{2}\binom{|S|}{2} \right| < \frac{1}{4}|S|^{2-\beta}.$$

In particular, this implies PaleyClique[α]. It is currently known that PaleyClique[1/2], although this was slightly improved in [1] for infinitely many p. It is widely conjectured that PaleyClique[ϵ] for every $\epsilon > 0$.

Our main theorem puts PaleyRIP[γ, η] in between these two classical conjectures.

Theorem 2.3 (Main Result)**.** *Each of the following statements implies the next:*

(a) *There exist* $0 < \alpha < 1/2$ *and* $0 < \beta < 2$ *such that* PaleyDiscrepancy[α, β].
(b) *There exist* $\gamma > 1/2$ *and* $\tau < 1/2$ *such that* PaleyRIP[$\gamma, \tau - 1/2 + \epsilon$] *for every* $\epsilon > 0$.
(c) *There exists* $\tau < 1/2$ *such that* PaleyClique[$\tau + \epsilon$] *for every* $\epsilon > 0$.

In particular, Conjecture 2.2 implies that Φ satisfies the (K, δ)-RIP with $K = \Omega(M^\gamma)$ for some $\gamma > 1/2$. As we will prove, it suffices to take any γ such that

$$\frac{1}{2} < \gamma < \min\left\{ \frac{1}{2-\beta}, \frac{1}{4\alpha} \right\}. \tag{2}$$

The optimal value of γ that this approach provides is given by maximizing (2) over α and with $\beta = \beta(\alpha)$ given by Conjecture 2.2. Since the optimal γ cannot be larger than 1, then as a byproduct of this theorem, we conclude that $\beta(\alpha) \le 1$ in Conjecture 2.2 whenever $\alpha < 1/4$.

We postpone the proof of the implication (a)⇒(b) to the next section; for now, we prove only the second implication.

Proof of (b)⇒(c) in Theorem 2.3. Let ω be the number of vertices in the largest clique of the Paley graph. We will show that $\omega \le \delta\sqrt{p}$, which will prove the claim since $\delta = p^{\tau - 1/2 + \epsilon}$. Let $\mathcal{K} \subset \mathbb{F}_p$ be a clique of maximal size, and let $a \in \mathbb{F}_p$ be a non-square (so that $\chi(a) = -1$). Then $\mathcal{I} := a\mathcal{K}$ is an independent set with cardinality ω, i.e., $\chi(i-j) = -1$ for every $i, j \in \mathcal{I}$ with $i \ne j$.

Let $\varphi_0, \dots, \varphi_p$ be the columns of Φ, and let $\Phi_\mathcal{I}$ denote the submatrix of Φ containing the columns $\{\varphi_i : i \in \mathcal{I}\}$. For any $i, j \in \mathbb{F}_p$ with $i \ne j$, we have

$$\langle \varphi_i, \varphi_j \rangle = \frac{1}{p} + \frac{2}{p}\sum_{x=1}^{p-1} 1_Q(x) \exp\big(-x(i-j)\big) = \frac{1}{p}\sum_{y=0}^{p-1} \exp\big(-y^2(i-j)\big), \tag{3}$$

where Q is the set of squares in $\mathbb{F}_p$, and the second equality follows from the fact that each nonzero $x \in Q$ has exactly two representations as $x = y^2$. The last sum in (3) is a well-known quadratic Gauss sum, which equals $p^{1/2}\chi(i-j)$ for $p \equiv 1 \bmod 4$. Thus, we get

$$\langle \varphi_i, \varphi_j \rangle = \frac{1}{\sqrt{p}}\chi(i-j) \tag{4}$$

In particular, if $i, j \in \mathcal{I}$ and $i \ne j$ then $\langle \varphi_i, \varphi_j \rangle = -p^{-1/2}$. This implies that

$$\Phi_\mathcal{I}^* \Phi_\mathcal{I} = (1 + p^{-1/2})I_\omega - p^{-1/2} J_\omega,$$

where I_ω denotes the $\omega \times \omega$ identity matrix and J_ω denotes the matrix of all 1s. The smallest eigenvalue of this matrix is $1 - \omega p^{-1/2}$.

By assumption, Φ satisfies the (p^γ, δ)-RIP. Since $|\mathcal{I}| = |\mathcal{K}| = \omega \le p^{1/2} \le p^\gamma$, we therefore have that the eigenvalues of $\Phi_\mathcal{I}^* \Phi_\mathcal{I}$ lie between $1 - \delta$ and $1 + \delta$. In particular, $1 - \omega p^{-1/2} \ge 1 - \delta$, and so rearranging gives $\omega \le \delta\sqrt{p}$, as desired. □

3. The Paley matrix satisfies the RIP

In this section, we give a proof of the implication (a)⇒(b) in Theorem 2.3. In order to show that Φ satisfies the RIP, we will employ a trick developed in [6] and show that Φ satisfies the so-called flat RIP property:

Definition 3.1. *An $M \times N$ matrix Φ with columns $\varphi_1, \dots, \varphi_N$ satisfies the (K, θ)-flat RIP if for every disjoint sets $I, J \subset [N]$ such that $|J| \leq |I| \leq K$, we have*

$$\left| \left\langle \sum_{i \in I} \varphi_i, \sum_{j \in J} \varphi_j \right\rangle \right| \leq \theta \sqrt{|I||J|}$$

The relation between flat RIP and RIP is given by the following proposition:

Proposition 3.2. *If Φ satisfies the (K, θ)-flat RIP and its columns have unit norm, then it satisfies the (K, δ)-RIP with $\delta = 150\theta \log K$.*

This proposition is essentially contained in [6], and follows from combining Lemma 11 with Theorem 13 from [4]. We will need a lemma to turn the sum of the type (1) into a sum over two disjoint sets, which flat RIP uses.

Lemma 3.3. *Let $p \equiv 1 \bmod 4$ be a prime and let $\alpha > 0$ and $0 < \beta < 2$ be such that (1) holds. Then for any $\tau \geq 2\alpha/(2-\beta)$, we have*

$$\left| \sum_{i \in I, j \in J} \chi(i-j) \right| \leq p^\tau \sqrt{3|I||J|} \tag{5}$$

for any disjoint sets $I, J \subset \mathbb{F}_p$ with $|J| \leq |I| \leq p^{2\tau/(2-\beta)}$.

Proof. The idea is to apply (1) three times: with $S = I$, $S = J$ and $S = I \cup J$. First observe that if $|I||J| \leq 3p^{2\tau}$, then we can apply the fact that $|\chi(x)| \leq 1$ for all $x \in \mathbb{F}_p$ together with the triangle inequality to get the trivial bound:

$$\left| \sum_{i \in I, j \in J} \chi(i-j) \right| \leq |I||J| \leq \sqrt{3p^{2\tau}} \sqrt{|I||J|} = p^\tau \sqrt{3|I||J|}.$$

Thus, we will assume that

$$|I||J| > 3p^{2\tau} \tag{6}$$

In particular $|I| > p^\tau$. Next, we consider the identity

$$\sum_{a,b \in I \cup J} \chi(a-b) = \sum_{a,b \in I} \chi(a-b) + \sum_{a,b \in J} \chi(a-b) + \sum_{i \in I, j \in J} \Big(\chi(i-j) + \chi(j-i) \Big).$$

Since $p \equiv 1 \bmod 4$, for every $x \in \mathbb{F}_p$ we have $\chi(-x) = \chi(x)$. Thus, it follows from the triangle inequality that

$$2 \left| \sum_{i \in I, j \in J} \chi(i-j) \right| \leq \left| \sum_{a,b \in I \cup J} \chi(a-b) \right| + \left| \sum_{a,b \in I} \chi(a-b) \right| + \left| \sum_{a,b \in J} \chi(a-b) \right|.$$

Applying (1) with $S = I$ and again with $S = I \cup J$ (observing that $\tau > \alpha$, and so $|I \cup J| \geq |I| > p^\tau > p^\alpha$) we get

$$2 \left| \sum_{i \in I, j \in J} \chi(i-j) \right| \leq |I \cup J|^{2-\beta} + |I|^{2-\beta} + \left| \sum_{a,b \in J} \chi(a-b) \right|. \tag{7}$$

We now deal with the sum over J. If $|J| \leq p^\alpha$ we use the triangle inequality and, recalling the bound imposed on τ, obtain

$$\left| \sum_{a,b \in J} \chi(a-b) \right| \leq |J|^2 \leq p^{2\alpha} \leq p^{\tau(2-\beta)} \leq |I|^{2-\beta}.$$

If $|J| > p^\alpha$, then we can apply (1) with $S = J$, and again we get

$$\left| \sum_{a,b \in J} \chi(a-b) \right| \leq |J|^{2-\beta} \leq |I|^{2-\beta}.$$

Plugging this back into (7) and using the fact that $|I \cup J| \leq 2|I|$, we get

$$\left| \sum_{i \in I, j \in J} \chi(i-j) \right| \leq \frac{1}{2}|I \cup J|^{2-\beta} + |I|^{2-\beta} \leq \left(\frac{2^{2-\beta}}{2} + 1 \right) |I|^{2-\beta} < 3|I|^{2-\beta}.$$

Finally, from the bound imposed on $|I|$, it follows that

$$\left| \sum_{i \in I, j \in J} \chi(i-j) \right| < 3|I|^{2-\beta} \leq 3p^{2\tau} = p^\tau \sqrt{9p^{2\tau}} \leq p^\tau \sqrt{3|I||J|},$$

where the last inequality follows from (6). □

We are now ready to prove the implication (a)⇒(b) of Theorem 2.3:

Proof of (a)⇒(b) in Theorem 2.3. Given PaleyDiscrepancy$[\alpha, \beta]$, take p large enough so that (1) holds. We will assume without loss of generality that $\beta \leq 1$, since otherwise, we may take $\beta = 1$ and (1) still holds. Fix γ satisfying (2). We proceed by considering two cases:

Case I. $\frac{2\alpha}{2-\beta} < \frac{1}{2}$.

In this case, we pick

$$\tau = \max\left\{ \frac{2\alpha}{2-\beta}, \frac{2-\beta}{2}\gamma \right\}$$

and $K = p^{2\tau/(2-\beta)}$. It is easily verified from (2) that $\tau < 1/2$ and $K \geq p^\gamma$.

To show that the Paley matrix Φ satisfies the RIP, we will employ Proposition 3.2 and show instead that it satisfies the flat RIP. We index the columns of Φ by $\{0, 1, \ldots, p\}$. Let I, J be disjoint subsets of $\{0, 1, \ldots, p\}$ with $|J| \leq |I| \leq K$. Suppose first that $p \notin I \cup J$, so that actually $I, J \subset \mathbb{F}_p$. Appealing to (4), we have

$$\left| \left\langle \sum_{i \in I} \varphi_i, \sum_{j \in J} \varphi_j \right\rangle \right| = \left| \sum_{i \in I, j \in J} \langle \varphi_i, \varphi_j \rangle \right| = \frac{1}{\sqrt{p}} \left| \sum_{i \in I, j \in J} \chi(i-j) \right| \leq p^{\tau - 1/2} \sqrt{3|I||J|}, \tag{8}$$

where the last step is by Lemma 3.3. Next, consider the case where $p \in J$ (the case $p \in I$ is analogous). Recalling that the last column of Φ is $\varphi_p = [1, 0, \ldots, 0]^\top$, we have

$$\left| \left\langle \sum_{i \in I} \varphi_i, \sum_{j \in J} \varphi_j \right\rangle \right| \leq \left| \left\langle \sum_{i \in I} \varphi_i, \sum_{j \in J \setminus \{p\}} \varphi_j \right\rangle \right| + \left| \left\langle \sum_{i \in I} \varphi_i, \varphi_p \right\rangle \right| = \left| \left\langle \sum_{i \in I} \varphi_i, \sum_{j \in J \setminus \{p\}} \varphi_j \right\rangle \right| + \frac{|I|}{\sqrt{p}}.$$

Observe that since $\beta \leq 1$, $|I| \leq \sqrt{|I|} p^{\tau/(2-\beta)} \leq \sqrt{|I|} p^\tau \leq p^\tau \sqrt{3|I||J|}$. Putting this together with (8), we get

$$\left| \left\langle \sum_{i \in I} \varphi_i, \sum_{j \in J} \varphi_j \right\rangle \right| \leq p^{\tau - 1/2} \sqrt{3|I||J|} + \frac{|I|}{\sqrt{p}} \leq 2p^{\tau - 1/2} \sqrt{3|I||J|}.$$

It follows that Φ satisfies the (K,θ)-flat RIP with $\theta = 2\sqrt{3}p^{\tau-1/2}$ and $K = p^{2\tau/(2-\beta)} \geq p^{\gamma}$. By Proposition 3.2, we conclude that Φ satisfies the (K,δ)-RIP with

$$\delta = 150\theta \log K = 300\sqrt{3}p^{\tau-1/2} \cdot \frac{2\tau}{2-\beta} \log p \leq p^{\tau-1/2+\epsilon},$$

where the last inequality holds for sufficiently large p.

Case II. $\frac{2\alpha}{2-\beta} \geq \frac{1}{2}$.

For this case, we will make β smaller so that the inequality reverts to the previous case. More precisely, pick γ^* such that

$$\gamma < \gamma^* < \min\left\{\frac{1}{2-\beta}, \frac{1}{4\alpha}\right\},$$

and pick $\beta^* = 2 - 1/\gamma^*$. Since $\gamma^* < 1/(2-\beta)$, we get $\beta^* < \beta$ and hence (1) still holds for β^*. Since $\gamma < \gamma^*$, the inequality (2) still holds when β is replaced by β^*. Since $\gamma^* < 1/(4\alpha)$, we have $\frac{2\alpha}{2-\beta^*} < \frac{1}{2}$. Therefore, one may use the same proof as the previous case, but using β^* in the place of β (and using the same γ). □

References

[1] C. Bachoc, I. Z. Ruzsa, M. Matolcsi, Squares and difference sets in finite fields, Available online: arXiv:1305.0577

[2] A. S. Bandeira, E. Dobriban, D. G. Mixon, W. F. Sawin, Certifying the restricted isometry property is hard, IEEE Trans. Inform. Theory 59 (2013) 3448–3450.

[3] A. S. Bandeira, M. Fickus, D. G. Mixon, J. Moreira, Derandomizing restricted isometries via the Legendre symbol, Available online: arXiv:1406.4089

[4] A. S. Bandeira, M. Fickus, D. G. Mixon, P. Wong, The road to deterministic matrices with the restricted isometry property, J. Fourier Anal. Appl. 19 (2013) 1123–1149.

[5] R. Baraniuk, M. Davenport, R. DeVore, M. Wakin, A simple proof of the restricted isometry property for random matrices, Constr. Approx. 28 (2008) 253–263.

[6] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, D. Kutzarova, Explicit contractions of RIP matrices and related problems, Duke Math. J. 159 (2011) 145–185.

[7] E. Candès, The restricted isometry property and its implications for compressed sensing, C. R. Math. Acad. Sci. Paris 346 (2008) 589–592.

[8] F. Chung, Several generalizations of Weil's sums, J. Number Theory 49 (1994) 95–106.

[9] F. Krahmer, S. Mendelson, H. Rauhut, Suprema of chaos processes and the restricted isometry property, Comm. Pure Appl. Math. 67 (2014) 1877–1904.

[10] D. G. Mixon, Explicit matrices with the restricted isometry property: Breaking the square-root bottleneck, Available online: arXiv:1403.3427

[11] J. Nelson, E. Price, M. Wootters, New constructions of RIP matrices with fast multiplication and fewer rows, SODA 2014, 1515–1528.

[12] H. Rauhut, Compressive sensing and structured random matrices, Theoretical foundations and numerical methods for sparse recovery 9 (2010) 1–92.

[13] M. Rudelson, R. Vershynin, On sparse reconstruction from Fourier and Gaussian measurements, Comm. Pure Appl. Math. 61 (2008) 1025–1045.

[14] T. Tao, Open question: Deterministic UUP matrices, Available online: `http://terrytao.wordpress.com/2007/07/02/open-question-deterministic-uup-matrices/`

[15] D. Zuckerman, General weak random sources, 31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990), 534–543, IEEE Comput. Soc. Press, Los Alamitos, CA, 1990.

(Bandeira) Program in Applied and Computational Mathematics, Princeton University, Princeton, NJ, USA (`ajsb@math.princeton.edu`).

(Mixon) Department of Mathematics and Statistics, Air Force Institute of Technology, Dayton, OH, USA (`dustin.mixon@afit.edu`).

(Moreira) Department of Mathematics, Ohio State University, Columbus, OH, USA (`moreira@math.osu.edu`).